Construction of Some Unimodular Lattices
with Long Shadows

Masaaki Harada[*]

January 18, 2013

Dedicated to Professor Yasumasa Nishiura on His 60th Birthday

Abstract

In this paper, we construct odd unimodular lattices in dimensions $n = 36, 37$ having minimum norm 3 and $4s = n - 16$, where s is the minimum norm of the shadow. We also construct odd unimodular lattices in dimensions $n = 41, 43, 44$ having minimum norm 4 and $4s = n - 24$.

1   Introduction

Shadows of odd unimodular lattices appeared in [5] (see also [6, p. 440]), and shadows play an important role in the study of odd unimodular lattices. Let L be an odd unimodular lattice in dimension n. The *shadow* $S(L)$ of L is defined to be $S(L) = L_0^* \setminus L$, where L_0 denotes the even sublattice of L and L_0^* denotes the dual lattice of L_0. Note that the norm of a vector of $S(L)$ is congruent to $n/4$ modulo 2 [5].

We define
$$\sigma(L) = 4 \min(S(L)),$$
where $\min(S(L))$ denotes the minimum norm of $S(L)$. Elkies [8] began the investigation of odd unimodular lattices L with long shadows, that is, large

---

[*]Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan, and PRESTO, Japan Science and Technology Agency (JST), Kawaguchi, Saitama 332–0012, Japan. email: mharada@sci.kj.yamagata-u.ac.jp

$\sigma(L)$. It was shown in [8] that $\sigma(L) \leq n$ and $\mathbb{Z}^n$ is the only odd unimodular lattice L with $\sigma(L) = n$, up to isomorphism. For the case $\sigma(L) < n$, we may assume that L has minimum norm at least 2 (see [9, 15]). Elkies [9] determined all such lattices for the case $\sigma(L) = n - 8$.

For the next case $\sigma(L) = n - 16$, Nebe and Venkov [15] showed that if there is an odd unimodular lattice L with minimum norm $\min(L) \geq 3$ then $n \leq 46$. Moreover, in this case, it is not known whether there is such a lattice with minimum norm 3 or not for only $n = 36, 37, 38, 39, 41, 42, 43$ (see [10, p. 148] and Table 1). It follows from [15, Table 1] that there is no odd unimodular lattice L with $\min(L) \geq 4$ for the case $\sigma(L) = n - 16$ (see also [11, Table 2]).

For the case $\sigma(L) = n - 24$, Gaborit [10] showed that if there is an odd unimodular lattice L with $\min(L) = 4$ then $n \leq 47$ (see also [11, Table 2]). Moreover, in this case, it is not known whether there is such a lattice or not for only $n = 37, 41, 43, 44, 45$ (see [10, p. 148] and Table 2).

The aim of this paper is to provide the existence of some unimodular lattices with long shadows whose existences were previously not known. These lattices are constructed from self-dual $\mathbb{Z}_k$-codes ($k = 4, 5$). The paper is organized as follows. In Section 2, we give definitions and some basic results on unimodular lattices and self-dual $\mathbb{Z}_k$-codes. In Section 3, we give conditions to construct odd unimodular lattices L in dimension 36 with $\min(L) = 3$ and $\sigma(L) = 20$ using self-dual $\mathbb{Z}_4$-codes by Construction A (Proposition 3.2). By finding a self-dual $\mathbb{Z}_4$-code satisfying these conditions, the first example of such a lattice is constructed. This dimension is the smallest dimension of an odd unimodular lattice L with $\min(L) = 3$ and $\sigma(L) = n - 16$ whose existence was previously not known. A new odd unimodular lattice L in dimension 36 with $\min(L) = 4$ and $\sigma(L) = 12$ is constructed as a neighbor of the above lattice. In Section 4, by considering self-dual $\mathbb{Z}_k$-codes ($k = 4, 5$), we construct an odd unimodular lattice L in dimension n with

$$(n, \min(L), \sigma(L)) = (37, 3, n - 16), (41, 4, n - 24), (43, 4, n - 24), \text{ and}$$
$$(44, 4, n - 24).$$

The current state of knowledge about the existence of unimodular lattices L in dimension n with $(\min(L), \sigma(L)) = (3, n - 16)$ and $(4, n - 24)$ is listed in Tables 1 and 2, respectively. All computer calculations in this paper were done by MAGMA [2].

2 Preliminaries

2.1 Unimodular lattices

A (Euclidean) lattice $L \subset \mathbb{R}^n$ in dimension n is *unimodular* if $L = L^*$, where the dual lattice L^* of L is defined as $\{x \in \mathbb{R}^n \mid (x, y) \in \mathbb{Z} \text{ for all } y \in L\}$ under the standard inner product (x, y). A unimodular lattice L is *even* if the norm (x, x) of every vector x of L is even and *odd* otherwise. An even unimodular lattice in dimension n exists if and only if $n \equiv 0 \pmod 8$, while an odd unimodular lattice exists for every dimension. The minimum norm $\min(L)$ of L is the smallest norm among all nonzero vectors of L. Two lattices L and L' are *isomorphic*, if there exists an orthogonal matrix A with $L' = L \cdot A = \{xA \mid x \in L\}$. The automorphism group of L is the group of all orthogonal matrices A with $L = L \cdot A$.

The theta series $\theta_L(q)$ of L is the formal power series $\theta_L(q) = \sum_{x \in L} q^{(x,x)}$. The kissing number is the second nonzero coefficient of the theta series, that is, the number of vectors of minimum norm in L. Conway and Sloane [5] showed that when the theta series of an odd unimodular lattice L in dimension n is written as

$$(1) \qquad \theta_L(q) = \sum_{j=0}^{\lfloor n/8 \rfloor} a_j \theta_3(q)^{n-8j} \Delta_8(q)^j,$$

the theta series of the shadow $S(L)$ is written as

$$(2) \qquad \theta_{S(L)}(q) = \sum_{j=0}^{\lfloor n/8 \rfloor} \frac{(-1)^j}{16^j} a_j \theta_2(q)^{n-8j} \theta_4(q^2)^{8j},$$

where $\Delta_8(q) = q \prod_{m=1}^{\infty} (1 - q^{2m-1})^8 (1 - q^{4m})^8$ and $\theta_2(q), \theta_3(q)$ and $\theta_4(q)$ are the Jacobi theta series [6].

2.2 Self-dual $\mathbb{Z}_k$-codes and Construction A

Let $\mathbb{Z}_k$ be the ring of integers modulo k, where k is a positive integer greater than 1. A $\mathbb{Z}_k$-*code* C of length n is a $\mathbb{Z}_k$-submodule of $\mathbb{Z}_k^n$. We shall exclusively deal with the case $k = 4$. Two $\mathbb{Z}_k$-codes are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. The *dual* code $C^\perp$ of C is defined as $C^\perp = \{x \in$

$\mathbb{Z}_k^n \mid x \cdot y = 0$ for all $y \in C\}$, where $x \cdot y = x_1 y_1 + \cdots + x_n y_n$ for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. A code C is *self-dual* if $C = C^\perp$. Let C be a self-dual $\mathbb{Z}_k$-code of length n. Then the following lattice

$$A_k(C) = \frac{1}{\sqrt{k}}\{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid (x_1 \bmod k, \ldots, x_n \bmod k) \in C\}$$

is a unimodular lattice in dimension n. This construction of lattices is called Construction A.

2.3 Self-dual $\mathbb{Z}_4$-codes

Let C denote a $\mathbb{Z}_4$-code of length n. The *Euclidean weight* of a codeword $x = (x_1, \ldots, x_n)$ of C is $n_1(x) + 4n_2(x) + n_3(x)$, where $n_\alpha(x)$ denotes the number of components i with $x_i = \alpha$ ($\alpha = 1, 2, 3$). The *minimum Euclidean weight* $d_E(C)$ of C is the smallest Euclidean weight among all nonzero codewords of C. Every $\mathbb{Z}_4$-code C of length n has two binary codes $C^{(1)}$ and $C^{(2)}$ associated with C:

$$C^{(1)} = \{c \bmod 2 \mid c \in C\} \text{ and } C^{(2)} = \{c \bmod 2 \mid c \in \mathbb{Z}_4^n, 2c \in C\}.$$

The binary codes $C^{(1)}$ and $C^{(2)}$ are called the *residue* and *torsion* codes of C, respectively. If C is self-dual, then $C^{(1)}$ is a binary doubly even code with $C^{(2)} = C^{(1)\perp}$ [4]. It is easy to see that $\min\{d(C^{(1)}), 4d(C^{(2)}))\} \leq d_E(C)$, where $d(C^{(i)})$ denotes the minimum weight of $C^{(i)}$ ($i = 1, 2$). In addition, $d_E(C) \leq 4d(C^{(2)})$ (see [12]). Also, $A_4(C)$ has minimum norm $\min\{4, d_E(C)/4\}$ (see [1]). Therefore, if $A_4(C)$ has minimum norm 3 (resp. 4), then C must have minimum Euclidean weight 12 (resp. at least 16) and $C^{(2)}$ has minimum weight at least 3 (resp. at least 4).

Two $\mathbb{Z}_4$-codes differing by only a permutation of coordinates are called permutation-equivalent. Any self-dual $\mathbb{Z}_4$-code C of length n with residue code of dimension k_1 is permutation-equivalent to a code C' with generator matrix in standard form

(3)
$$\begin{pmatrix} I_{k_1} & A & B_1 + 2B_2 \\ O & 2I_{n-2k_1} & 2D \end{pmatrix},$$

where A, B_1, B_2, D are $(1,0)$-matrices, I_k denotes the identity matrix of order k, and O denotes the zero matrix [4]. In this paper, when we give a generator matrix of C, we consider a generator matrix in standard form (3)

of C', which is permutation-equivalent to C, then we only list the $k_1 \times (n-k_1)$ matrix $\begin{pmatrix} A & B_1 + 2B_2 \end{pmatrix}$ to save space. Note that $\begin{pmatrix} O & 2I_{n-2k_1} & 2D \end{pmatrix}$ in (3) can be obtained from $\begin{pmatrix} I_{k_1} & A & B_1 + 2B_2 \end{pmatrix}$ since $C'^{(2)} = C'^{(1)\perp}$.

3   Dimension $n = 36$ and $\sigma(L) = n - 16, n - 24$

In this section, we give conditions to construct odd unimodular lattices L in dimension $n = 36$ with $\min(L) = 3$ and $\sigma(L) = n - 16$ from self-dual $\mathbb{Z}_4$-codes by Construction A. By finding a self-dual $\mathbb{Z}_4$-code satisfying these conditions, the first example of such a lattice is constructed. A new optimal odd unimodular lattice L with $\sigma(L) = n - 24$ is also constructed from the above lattice.

Let L_{36} be an odd unimodular lattice in dimension 36 having minimum norm at least 3. Using (1) and (2), it is easy to determine the possible theta series $\theta_{L_{36}}(q)$ and $\theta_{S(L_{36})}(q)$ of L_{36} and its shadow $S(L_{36})$:

$$
\begin{aligned}
\theta_{L_{36}}(q) = &1 + (960 - \alpha)q^3 + (42840 + 4096\beta)q^4 \\
&\qquad\qquad + (1882368 + 36\alpha - 98304\beta)q^5 + \cdots , \\
\theta_{S(L_{36})}(q) = &\beta q + (\alpha - 60\beta)q^3 + (3833856 - 36\alpha + 1734\beta)q^5 + \cdots ,
\end{aligned}
$$

respectively, where α and β are nonnegative integers. Then, the following lemma is immediate.

Lemma 3.1. *Let L be an odd unimodular lattice in dimension 36 having minimum norm 3. Then, the kissing number of L is at most 960, and the equality holds if and only if $\sigma(L) = 20$.*

Now, we give a method for construction of unimodular lattices $A_4(C)$ with $\min(A_4(C)) = 3$ and $\sigma(A_4(C)) = 20$, using self-dual $\mathbb{Z}_4$-codes C. It is known that a binary $[36, k, 3]$ code exists only if $k \leq 30$ (see [3]). Hence, the dimension of the residue code of a self-dual $\mathbb{Z}_4$-code of length 36 and minimum Euclidean weight 12 is at least 6.

Proposition 3.2. *Let C be a self-dual $\mathbb{Z}_4$-code of length 36 such that $C^{(1)}$ is a binary doubly even $[36, 6, 16]$ code and $C^{(2)}$ has minimum weight 3. Then $A_4(C)$ is a unimodular lattice with $\min(A_4(C)) = 3$ and $\sigma(A_4(C)) = 20$.*

5

Proof. Let B be a binary doubly even $[36, 6, 16]$ code such that $B^\perp$ has minimum weight 3. The weight enumerator of B is written as:

$$W_B(y) = 1 + ay^{16} + by^{20} + cy^{24} + dy^{28} + ey^{32} + (2^6 - 1 - a - b - c - d - e)y^{36},$$

where a, b, c, d and e are nonnegative integers. Since $B^\perp$ contains a codeword of weight 3, $2^6 - 1 - a - b - c - d - e = 0$. By the MacWilliams identity, the weight enumerator of $B^\perp$ is given by:

$$\begin{aligned} W_{B^\perp}(y) = &1 + \frac{1}{8}(-216 + 4a + 3b + 2c + d)y + (378 - 6a - 6b - 5c - 3d)y^2 \\ &+ \frac{1}{8}(-24024 + 388a + 403b + 386c + 273d)y^3 + \cdots. \end{aligned}$$

Since $B^\perp$ has minimum weight 3, we have

$$c = 270 - 6a - 3b \text{ and } d = -324 + 8a + 3b.$$

Thus, the weight enumerators of B and $B^\perp$ are written using a and b:

$$\begin{aligned} W_B(y) = &1 + ay^{16} + by^{20} + (270 - 6a - 3b)y^{24} + (-324 + 8a + 3b)y^{28} \\ &+ (117 - 3a - b)y^{32}, \\ W_{B^\perp}(y) = &1 + (-1032 + 32a + 8b)y^3 + (17649 - 448a - 128b)y^4 + \cdots, \end{aligned}$$

respectively. Then, only $(a, b) = (27, 36)$ satisfies the condition that the above coefficients in $W_B(y)$ and $W_{B^\perp}(y)$ are nonnegative integers. Hence, the weight enumerators of B and $B^\perp$ are uniquely determined as

(4) $W_B(y) = 1 + 27y^{16} + 36y^{20},$

(5) $W_{B^\perp}(y) = 1 + 120y^3 + 945y^4 + 5832y^5 + 30576y^6 + 130680y^7 + \cdots,$

respectively.

As described in Section 2.3, we have

(6) $$\min\{d(C^{(1)}), 4d(C^{(2)}))\} \leq d_E(C) \leq 4d(C^{(2)}).$$

Hence, $d_E(C) = 12$ and $A_4(C)$ has minimum norm 3. Let e_i denote the i-th unit vector $(\delta_{i,1}, \delta_{i,2}, \ldots, \delta_{i,36})$, for $i = 1, 2, \ldots, 36$, where δ_{ij} is the Kronecker delta. By (5), there are 120 codewords of weight 3 in $C^{(2)}$, and we denote

the set of the 120 codewords by $C_3^{(2)}$. Then, $A_4(C)$ contains the following set of vectors of norm 3:

$$\{\pm e_{j_1} \pm e_{j_2} \pm e_{j_3} \mid \{j_1, j_2, j_3\} \in S\},$$

where $S = \{\mathrm{supp}(x) \mid x \in C_3^{(2)}\}$, and $\mathrm{supp}(x)$ denotes the support of x. Hence, there are at least 960 vectors of norm 3 in $A_4(C)$. By Lemma 3.1, the result follows. $\square$

It was shown in [16] that there are four inequivalent binary $[36, 7, 16]$ codes containing the all-one vector $\mathbf{1}$. Such a code and its dual code have the following weight enumerators:

$$1 + 63y^{16} + 63y^{20} + y^{36},$$
$$1 + 945y^4 + 30576y^6 + 471420y^8 + 3977568y^{10} + \cdots ,$$

respectively. Let $B_{36,7,1}$ denote the binary $[36, 7, 16]$ code containing $\mathbf{1}$ with automorphism group of order 1451520 which is the symplectic group $Sp(6, 2)$. Using an approach used in [13, Section 4], we verified that $B_{36,7,1}$ contains only one doubly even $[36, 6, 16]$ subcode $B_{36,6}$ such that $B_{36,6}^{\perp}$ has minimum weight 3 up to equivalence. The weight enumerators of $B_{36,6}$ and $B_{36,6}^{\perp}$ are given by (4) and (5), respectively. We verified by MAGMA that $B_{36,6}$ has automorphism group of order 51840 containing the symplectic group $Sp(4, 3)$ as a subgroup of index 2.

Starting from a given binary doubly even code B, a method for construction of all self-dual $\mathbb{Z}_4$-codes C with $C^{(1)} = B$ was given in [17, Section 3]. Using this method, we construct a self-dual $\mathbb{Z}_4$-code C_{36} with $C_{36}^{(1)} = B_{36,6}$ explicitly. By Proposition 3.2, $A_4(C_{36})$ is the desired unimodular lattice with $\sigma(A_4(C_{36})) = 20$, and we have the following:

Proposition 3.3. *There is a unimodular lattice L in dimension 36 having minimum norm 3 with $\sigma(L) = 20$.*

We verified by MAGMA that the unimodular lattice $A_4(C_{36})$ has automorphism group of order 1698693120. For the code C_{36}, we give a generator

matrix in standard form (3), by only listing the 6×30 matrix:

$$
\left(\begin{array}{cc} A & B_1 + 2B_2 \end{array} \right) = \left(\begin{array}{cc}
000010001011100111100010 & 130113 \\
011001000101000011101001 & 231133 \\
100010010111110001110111 & 000230 \\
110011100011001100111111 & 032133 \\
011110101100111001011001 & 321113 \\
111111111111110000000000 & 222203
\end{array} \right).
$$

There are three unimodular lattices containing the even sublattice of $A_4(C_{36})$. We denote the two unimodular lattices rather than $A_4(C_{36})$ by N_{36} and N'_{36}. It follows from the theta series of $A_4(C_{36})$ and $S(A_4(C_{36}))$ that both N_{36} and N'_{36} have minimum norm 4 and kissing number 42840, thus, $\sigma(N_{36}) = \sigma(N'_{36}) = 16$. We verified by MAGMA that the two lattices are isomorphic. We also verified by MAGMA that N_{36} has automorphism group of order 849346560, which is different to those of two previously known unimodular lattices with minimum norm 4 and kissing number 42840 in [14].

Let $C_{36,0}$ be the subcode of C_{36} consisting of codewords of Euclidean weight divisible by 8. Then $C_{36,0}$ is a subcode of index 2 in C_{36} (see [7, Lemma 3.1]). By Proposition 3.8 in [7], there is a self-dual $\mathbb{Z}_4$-code D_{36} containing $C_{36,0}$ with $A_4(D_{36}) = N_{36}$. For the code D_{36}, we give a generator matrix in standard form (3), by only listing the 6×30 matrix:

$$
\left(\begin{array}{cc} A & B_1 + 2B_2 \end{array} \right) = \left(\begin{array}{cc}
000110111001000100110 & 0131310 \\
110111100010100101010 & 1233122 \\
011110001111001010011 & 0121203 \\
111010011000111011011 & 3133300 \\
010100110110001101101 & 1203301 \\
000001111111111111110 & 0022113 \\
111111111111100000000 & 2220232
\end{array} \right).
$$

We verified that the residue code $D_{36}^{(1)}$ is equivalent to $B_{36,7,1}$.

Remark 3.4. The remaining three binary $[36, 7, 16]$ codes containing $\mathbf{1}$ have automorphism groups of orders 10752, 1920 and 672 [16]. We denote these codes by $B_{36,7,2}$, $B_{36,7,3}$ and $B_{36,7,4}$, respectively. We verified that $B_{36,7,2}$, $B_{36,7,3}$ and $B_{36,7,4}$ contain $1, 2$ and 1 doubly even $[36, 6, 16]$ subcodes such that the dual codes have minimum weight 3, respectively, up to equivalence, and the four codes and $B_{36,6}$ are inequivalent to each other. By Proposition 3.2, the four inequivalent codes rather than $B_{36,6}$ also give examples of unimodular lattices L with $\min(L) = 3$ and $\sigma(L) = 20$.

4   Other cases

4.1   Dimension $n = 37$ and $\sigma(L) = n - 16$

Let L_{37} be an odd unimodular lattice in dimension $n = 37$ having minimum norm at least 3. We give the possible theta series of L_{37} and its shadow $S(L_{37})$:

$$\theta_{L_{37}}(q) = 1 + (1184 - \alpha)q^3 + (37962 - 2\alpha + 2048\beta)q^4$$
$$+ (1758240 + 36\alpha - 45056\beta)q^5 + \cdots,$$
$$\theta_{S(L_{37})}(q) = \beta q^{5/4} + (2\alpha - 59\beta)q^{13/4} + (8486912 - 70\alpha + 1674\beta)q^{21/4} + \cdots,$$

respectively, where α and β are nonnegative integers. It turns out that L_{37} has minimum norm 3 and kissing number 1184 if and only if $\sigma(L_{37}) = 21$.

It is known that a binary $[37, k, 3]$ code exists only if $k \leq 31$ (see [3]). Hence, the dimension of the residue code of a self-dual $\mathbb{Z}_4$-code of length 37 and minimum Euclidean weight 12 is at least 6. When $n = 37$, we have a weaker result than Proposition 3.2.

Proposition 4.1. *Let B be a binary doubly even $[37, 6]$ code such that the dual code has minimum weight 3. Then the weight enumerator $W_B(y)$ of B is given by:*

(7) $W_B(y) = 1 + 20y^{16} + 42y^{20} + y^{24}$ *or,*

(8) $W_B(y) = 1 + y^{12} + 17y^{16} + 45y^{20}.$

Proof. The proof is similar to that of Proposition 3.2. Let B be a binary doubly even $[37, 6]$ code such that $B^{\perp}$ has minimum weight 3. The weight enumerator $W_B(y)$ is written as:

$$W_B(y) = 1 + ay^4 + by^8 + cy^{12} + dy^{16} + ey^{20} + fy^{24} + gy^{28}$$
$$+ hy^{32} + (2^6 - 1 - a - b - c - d - e - f - g - h)y^{36},$$

where a, b, c, d, e, f, g and h are nonnegative integers. Then the weight enu-

9

merator of $B^\perp$ is given by:

$$W_{B^\perp}(y) = 1 + \frac{1}{8}(-271 + 8a + 7b + 6c + 5d + 4e + 3f + 2g + h)y$$
$$+ \frac{1}{8}(4761 - 24a - 49b - 66c - 75d - 76e - 69f - 54g - 31h)y^2$$
$$+ \frac{1}{8}(-50295 + 1256a + 959b + 830c + 805d + 820e + 811f$$
$$+ 714g + 465h)y^3 + \cdots .$$

From the condition that $B^\perp$ has minimum weight 3, we have

$$g = 455 - 28a - 21b - 15c - 10d - 6e - 3f,$$
$$h = -639 + 48a + 35b + 24c + 15d + 8e + 3f.$$

Thus, the weight enumerators are written as:

$$W_B(y) = 1 + ay^4 + by^8 + cy^{12} + dy^{16} + ey^{20} + fy^{24}$$
$$+ (455 - 28a - 21b - 15c - 10d - 6e - 3f)y^{28}$$
$$+ (-639 + 48a + 35b + 24c + 15d + 8e + 3f)y^{32}$$
$$+ (247 - 21a - 15b - 10c - 6d - 3e - f)y^{36},$$
$$W_{B^\perp}(y) = 1 + (-2820 + 448a + 280b + 160c + 80d + 32e + 8f)y^3 + \cdots .$$

Then, only

$$(a, b, c, d, e, f) = (0, 0, 0, 20, 42, 1) \text{ and } (0, 0, 1, 17, 45, 0)$$

satisfy the condition that the coefficients in $W_B(y)$ are nonnegative integers. These cases correspond to (7) and (8), respectively. $\square$

For (7) and (8), $W_{B^\perp}(y)$ is given by:

(9) $W_{B^\perp}(y) = 1 + 132y^3 + 1072y^4 + 6705y^5 + 36324y^6 + \cdots ,$
(10) $W_{B^\perp}(y) = 1 + 140y^3 + 1080y^4 + 6633y^5 + 36252y^6 + \cdots ,$

respectively.

Corollary 4.2. *Let C be a self-dual $\mathbb{Z}_4$-code of length 37 such that $C^{(1)}$ is a binary doubly even $[37, 6, 12]$ code and $C^{(2)}$ has minimum weight 3. Then $A_4(C)$ is a unimodular lattice with $\min(A_4(C)) = 3$ and kissing number at least 1120.*

10

Proof. By (6), C has minimum Euclidean weight 12. It follows from (10) that $A_4(C)$ has at least 1120 vectors of norm 3. □

As a subcode of some binary maximal doubly even code of length 37, we found a doubly even $[37, 6, 12]$ code B_{37} such that $B_{37}^\perp$ has minimum weight 3. The weight enumerators of B_{37} and $B_{37}^\perp$ are given by (8) and (10), respectively. We verified by MAGMA that B_{37} has automorphism group of order 120 which is the symmetric group of degree 5.

Corollary 4.2 only guarantees that $A_4(C)$ has minimum norm 3 and kissing number at least 1120 for a self-dual $\mathbb{Z}_4$-code C with $C^{(1)} = B_{37}$. Using the method in [17, Section 3], we found a self-dual $\mathbb{Z}_4$-code C_{37} such that $C_{37}^{(1)} = B_{37}$ and the kissing number of $A_4(C_{37})$ is exactly 1184. Therefore, we have the following:

Proposition 4.3. *There is a unimodular lattice L in dimension* 37 *having minimum norm* 3 *with $\sigma(L) = 21$.*

We verified by MAGMA that the unimodular lattice $A_4(C_{37})$ has automorphism group of order 7864320. For the code C_{37}, we give a generator matrix in standard form (3), by only listing the 6×31 matrix:

$$
\begin{pmatrix} A & B_1 + 2B_2 \end{pmatrix} = \begin{pmatrix}
0101001010110011110000011 & 003121 \\
0111100111010100000110110 & 323200 \\
1010001100010011111110101 & 313301 \\
0000001110001100111101100 & 033031 \\
1110011111111010100000000 & 000132 \\
1001110010000111111111000 & 220010
\end{pmatrix}.
$$

4.2 Dimension $n = 41$ and $\sigma(L) = n - 24$

Let L_{41} be an odd unimodular lattice in dimension 41 having minimum norm 4. We give the possible theta series of L_{41} and its shadow $S(L_{41})$:

$$
\theta_{L_{41}}(q) = 1 + (15170 + 128\alpha)q^4 + (1226720 - 1792\alpha - 524288\beta)q^5 + \cdots ,
$$
$$
\theta_{S(L_{41})}(q) = \beta q^{1/4} + (\alpha - 79\beta)q^{9/4} + (104960 - 55\alpha + 3040\beta)q^{17/4} + \cdots ,
$$

respectively, where α and β are nonnegative integers. It turns out that L_{41} has kissing number 15170 if and only if $\sigma(L_{41}) = 17$.

Let C_{41} be the $\mathbb{Z}_4$-code with generator matrix in standard form (3), where $\begin{pmatrix} A & B_1 + 2B_2 \end{pmatrix}$ is listed in Figure 1. We verified that C_{41} is a self-dual $\mathbb{Z}_4$-code of minimum Euclidean weight 16 such that $A_4(C_{41})$ has kissing number 15170. Hence, we have the following:

Proposition 4.4. *There is a unimodular lattice L in dimension 41 having minimum norm 4 with $\sigma(L) = 17$.*

$$\begin{pmatrix} A & B_1 + 2B_2 \end{pmatrix} = \begin{pmatrix} 10111111111001000010001 & 101031013 \\ 11001100111111100111000 & 112233010 \\ 01101100001100110110100 & 001332012 \\ 11010101000111001010100 & 023102310 \\ 11111010110101011110111 & 033211301 \\ 10000101001101101010101 & 132003201 \\ 11100110011010001101111 & 210211330 \\ 01110001111111010000111 & 230321312 \\ 01101110010011001111011 & 232022022 \end{pmatrix}$$

Figure 1: Generator matrix of C_{41}

The residue code $C_{41}^{(1)}$ is a binary doubly even $[41, 9, 12]$ code with a trivial automorphism group and weight enumerator:

$$1 + y^{12} + 89y^{16} + 288y^{20} + 108y^{24} + 23y^{28} + 2y^{32}.$$

4.3 Dimension $n = 43$ and $\sigma(L) = n - 24$

Let L_{43} be an odd unimodular lattice in dimension 43 having minimum norm 4. We give the possible theta series of L_{43} and its shadow $S(L_{43})$:

$$\theta_{L_{43}}(q) = 1 + (9030 + 32\alpha)q^4 + (941184 - 320\alpha - 131072\beta)q^5 + \cdots,$$
$$\theta_{S(L_{43})}(q) = \beta q^{3/4} + (\alpha - 77\beta)q^{11/4} + (660480 - 53\alpha + 2883\beta)q^{19/4} + \cdots,$$

respectively, where α and β are nonnegative integers. It turns out that L_{43} has kissing number 9030 if and only if $\sigma(L_{43}) = 19$.

Let C_{43} be the $\mathbb{Z}_4$-code with generator matrix in standard form (3), where $\begin{pmatrix} A & B_1 + 2B_2 \end{pmatrix}$ is listed in Figure 2. We verified that C_{43} is a self-dual $\mathbb{Z}_4$-code of minimum Euclidean weight 16 such that $A_4(C_{43})$ has kissing number 9030. Hence, we have the following:

Proposition 4.5. *There is a unimodular lattice L in dimension 43 having minimum norm 4 with $\sigma(L) = 19$.*

$$
(\; A \quad B_1 + 2B_2 \;) = \begin{pmatrix}
01010011110100111 & 0033202030013 \\
01100001111010111 & 3212001202013 \\
10100011110100010 & 1122313032032 \\
00001111111011100 & 1100211211331 \\
01101101000000110 & 3300133330012 \\
00011011001111100 & 2213322021123 \\
00111011110010110 & 1230201103220 \\
00100000101001101 & 0121022213003 \\
11000010110100011 & 1012310010101 \\
01011101010110101 & 3321023022100 \\
10001011010111000 & 3021302111320 \\
00001000111100101 & 3231010323110 \\
11111111111111000 & 0222002002232
\end{pmatrix}
$$

Figure 2: Generator matrix of C_{43}

The residue code $C_{43}^{(1)}$ is a binary doubly even $[43, 13, 12]$ code with a trivial automorphism group and weight enumerator:

$$1 + 29y^{12} + 1067y^{16} + 3498y^{20} + 3010y^{24} + 569y^{28} + 18y^{32}.$$

4.4 Dimension $n = 44$ and $\sigma(L) = n - 24$

Let L_{44} be an odd unimodular lattice in dimension 44 having minimum norm 4. We give the possible theta series of L_{44} and its shadow $S(L_{44})$:

$$
\begin{aligned}
\theta_{L_{44}}(q) &= 1 + (6600 + 16\alpha)q^4 + (811008 - 128\alpha - 65536\beta)q^5 + \cdots, \\
\theta_{S(L_{44})}(q) &= \beta q + (\alpha - 76\beta)q^3 + (1622016 - 52\alpha + 2806\beta)q^5 + \cdots,
\end{aligned}
$$

respectively, where α and β are nonnegative integers. It turns out that L_{44} has kissing number 6600 if and only if $\sigma(L_{44}) = 20$.

Let C_{44} be the $\mathbb{F}_5$-code of length 44 whose generator matrix is

$$
\begin{pmatrix}
I_{22} & \begin{matrix} A & B \\ -B^T & A^T \end{matrix}
\end{pmatrix},
$$

13

where A and B are 11×11 negacirculant matrices with the first rows

$$(1, 0, 0, 0, 0, 3, 3, 0, 1, 0, 3) \text{ and } (0, 1, 1, 0, 2, 1, 0, 0, 0, 2, 3),$$

respectively, that is, A and B have the following form

$$\begin{pmatrix} r_1 & r_2 & r_3 & \cdots & r_{11} \\ -r_{11} & r_1 & r_2 & \cdots & r_{10} \\ -r_{10} & -r_{11} & r_1 & \cdots & r_9 \\ \vdots & \vdots & \vdots & & \vdots \\ -r_2 & -r_3 & -r_4 & \cdots & r_1 \end{pmatrix},$$

and A^T denotes the transposed matrix of A. Since $AA^T + BB^T = 4I_{11}$, C_{44} is self-dual. In addition, it can be checked that C_{44} has the following weight enumerator:

$$1 + 924y^{12} + 1848y^{13} + 19272y^{14} + 91168y^{15} + \cdots.$$

We verified by MAGMA that the unimodular lattice $A_5(C_{44})$ has minimum norm 4 and kissing number 6600. Hence, we have the following:

Proposition 4.6. *There is a unimodular lattice L in dimension 44 having minimum norm 4 with $\sigma(L) = 20$.*

Our computer search failed to discover a unimodular lattice with long shadow using a self-dual $\mathbb{Z}_4$-code for this case and the remaining cases that the existences are not known.

4.5 Summary

As a summary, we list the number $\#$ of known non-isomorphic unimodular lattices L in dimension n with $\min(L) = 3$ and $\sigma(L) = n - 16$ (resp. $\min(L) = 4$ and $\sigma(L) = n - 24$) in Table 1 (resp. Table 2). Both tables update the two tables given in [10, p. 148]. We remark that the existence of a unimodular lattice L in dimension 37 having minimum norm 4 is still unknown for any $\sigma(L)$ (see [14]).

Table 1: Unimodular lattices L with $\min(L) = 3$ and $\sigma(L) = n - 16$

n	#	References	n	#	References
23	1	(see [15])	35	≥ 1	[15]
24	1	(see [15])	36	≥ 1	$A_4(C_{36})$ in Section 3
25	0	(see [15])	37	≥ 1	$A_4(C_{37})$ in Section 4
26	1	(see [15])	38	?	
27	2	(see [15])	39	?	
28	36	(see [15])	40	≥ 1	(see [10])
29	≥ 1	[15]	41	?	
30	≥ 1	[15]	42	?	
31	≥ 1	[15]	43	?	
32	≥ 1	[15]	44	0	[15]
33	≥ 1	[15]	45	0	[15]
34	≥ 1	[15]	46	1	[15]

References

[1] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* **43** (1997), 969–976.

[2] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at http://magma.maths.usyd.edu.au/magma/.

[3] A.E. Brouwer, "Bounds on the size of linear codes," in Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 295–461.

[4] J.H. Conway and N.J.A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory Ser. A* **62** (1993), 30–45.

[5] J.H. Conway and N.J.A. Sloane, A note on optimal unimodular lattices, *J. Number Theory* **72** (1998), 357–362.

[6] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups (3rd ed.)*, Springer-Verlag, New York, 1999.

[7] S.T. Dougherty, M. Harada and P. Solé, Shadow codes over $\mathbb{Z}_4$, *Finite Fields Appl.* **7** (2001), 507–529.

Table 2: Unimodular lattices L with $\min(L) = 4$ and $\sigma(L) = n - 24$

n	#	References	n	#	References
32	5	[5]	42	≥ 1	(see [10])
36	≥ 3	[14], $A_4(D_{36})$ in Section 3	43	≥ 1	$A_4(C_{43})$ in Section 4
37	?		44	≥ 1	$A_5(C_{44})$ in Section 4
38	≥ 1	(see [10])	45	?	
39	≥ 1	(see [10])	46	≥ 1	(see [10])
40	≥ 1	(see [10])	47	≥ 1	(see [10])
41	≥ 1	$A_4(C_{41})$ in Section 4			

[8] N.D. Elkies, A characterization of the $\mathbb{Z}^n$-lattice, *Math. Research Letters* **2** (1995), 321–326.

[9] N.D. Elkies, Lattices and codes with long shadows, *Math. Research Letters* **2** (1995), 643–651.

[10] P. Gaborit, A bound for certain s-extremal lattices and codes, *Arch. Math.* **89** (2007), 143–151.

[11] M. Gaulter, Characteristic vectors of unimodular lattices which represent two, *J. Theór. Nombres Bordeaux* **19** (2007), 405–414.

[12] M. Harada, Extremal Type II $\mathbb{Z}_4$-codes of lengths 56 and 64, *J. Combin. Theory Ser. A* **117** (2010), 1285–1288.

[13] M. Harada, C.H. Lam and A. Munemasa, On the structure codes of the moonshine vertex operator algebra, (submitted), ArXiv:math.QA/1005.1144.

[14] G. Nebe and N.J.A. Sloane, Unimodular lattices, together with a table of the best such lattices, in *A Catalogue of Lattices*, published electronically at `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/`.

[15] G. Nebe and B. Venkov, Unimodular lattices with long shadow, *J. Number Theory* **99** (2003), 307–317.

[16] C. Parker, E. Spence and V.D. Tonchev, Designs with the symmetric difference property on 64 points and their groups, *J. Combin. Theory Ser. A* **67** (1994), 23–43.

[17] V. Pless, J. Leon and J. Fields, All $\mathbb{Z}_4$ codes of Type II and length 16 are known, *J. Combin. Theory Ser. A* **78** (1997), 32–50.